

**ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»**

Циклова комісія економіки, управління та адміністрування

Заїкін Роман Михайлович

ПІБ здобувача

КУРСОВА РОБОТА

**Впровадження сучасних цифрових технологій в управління фінансово-
економічною безпекою**

тема

Навчальна
дисципліна

Фінансово-економічна безпека організації

назва навчальної дисципліни

Ступінь освіти

Фаховий молодший бакалавр

фаховий молодший бакалавр, молодший бакалавр, бакалавр

Галузь знань

07 Управління та адміністрування

шифр і назва галузі знань

Спеціальність

**072 Фінанси, банківська справа, страхування та
фондовий ринок**

код і найменування спеціальності

Освітньо-професійна
програма

Фінанси і кредит

назва освітньо-професійної програми

Академічна група

Ф-24

назва академічної групи

Харків, 2026 рік

Керівник:

Постольна Наталія Олександрівна, викладач
циклової комісії економіки, управління та
адміністрування, спеціаліст вищої категорії

Робота містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач

підпис здобувача

Заїкін Р.М.

ПІБ здобувача

Підсумкова оцінка: **70** (балів)

Члени комісії з захисту:

(підпис)

Н. О. Постольна

(підпис)

О.М. Тимошенко

**ВСП «Харківський торговельно-економічний фаховий коледж
Державного торговельно-економічного університету»**

Циклова комісія економіки, управління та адміністрування

Заїкін Роман Михайлович

ПІБ здобувача

ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Навчальна
дисципліна

Фінансово-економічна безпека організації

назва навчальної дисципліни

Тема роботи

Впровадження сучасних цифрових технологій в
управління фінансово-економічною безпекою

тема курсової роботи

Термін подання
завершеної роботи

26.04.2026 р.

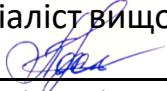
фаховий молодший бакалавр, молодший бакалавр, бакалавр

Графік виконання роботи

Виконання роботи за розділами	Термін виконання
Вибір та затвердження теми	02.02 – 08.02.2026
Добір та аналіз літератури за обраною темою	09.02 – 15.02.2026
Складання плану курсової роботи	16.02 – 22.02.2026
Написання вступу та I розділу	23.02 – 15.03.2026
Написання розрахункової частини (II розділ) курсової роботи	16.03 – 05.04.2026
Написання висновків та пропозицій, оформлення курсової роботи	06.04 – 19.04.2026
Подання курсової роботи керівнику для рецензування (для рекомендації до захисту)	20.04 – 26.04.2026
Захист курсової роботи	04.05 – 09.05.2026

Завдання видав

Науковий керівник,
спеціаліст вищої категорії


Наталія ПОСТОЛЬНА
(підпис)

«02» лютого 2026 р.

Завдання отримав

Здобувач


Роман ЗАЙКІН .
(підпис) ПІБ здобувача

«02» лютого 2026 р.

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1. СУЧАСНІ ЦИФРОВІ ТЕХНОЛОГІЇ В УПРАВЛІННІ БЕЗПЕКОЮ.....	6
1.1. Поняття та класифікація цифрових технологій	6
1.2. Використання великих даних, аналітики та штучного інтелекту	7
1.3. Роль блокчейн-технологій у забезпеченні безпеки та кібербезпеки як складових фінансово-економічної безпеки	9
РОЗДІЛ 2. ОЦІНКА СТАНУ ФІНАНСОВОЇ БЕЗПЕКИ ТОВ «АТБ-МАРКЕТ» ТА ШЛЯХИ ЇЇ ПІДВИЩЕННЯ.....	12
2.1. Характеристика діяльності підприємства	12
2.2. Аналіз фінансової безпеки підприємства та виявлення слабких місць у системі управління	13
2.3. Методи вдосконалення управління фінансово-економічною безпекою підприємства	16
ВИСНОВКИ	18
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	20

ВСТУП

У сучасних умовах розвитку цифрової економіки підприємства функціонують в середовищі підвищеної нестабільності, що супроводжується посиленням конкуренції, глобалізацією ринків та зростанням кількості економічних і фінансових ризиків. Відповідно до теоретичних положень економічної безпеки, ефективне функціонування підприємства можливе лише за умови забезпечення належного рівня фінансово-економічної безпеки, яка охоплює захист ресурсів, стабільність розвитку та здатність протидіяти загрозам.

Фінансово-економічна безпека підприємства визначається як стан захищеності його фінансових інтересів, що забезпечує стабільне функціонування та розвиток у довгостроковій перспективі. Вона формується під впливом як зовнішніх, так і внутрішніх факторів. До зовнішніх належать макроекономічні умови, державна політика, рівень інфляції, валютна стабільність, а також інвестиційний клімат. Внутрішні фактори включають ефективність управління, фінансову стійкість, рівень ліквідності та організацію системи ризик-менеджменту.

Згідно з матеріалами лекцій, фінансово-економічна безпека розглядається на макро- та мікрорівнях. Макрорівень охоплює економічну стабільність держави, ефективність податкової та кредитної політики, рівень корупції та розвиток фінансових ринків. Мікрорівень відображає стан конкретного підприємства та залежить від його фінансової стратегії, здатності управляти ризиками і забезпечувати платоспроможність.

Особливої актуальності набуває впровадження сучасних цифрових технологій, які суттєво трансформують підходи до управління фінансово-економічною безпекою. Використання великих даних (Big Data), аналітичних систем, штучного інтелекту та блокчейн-технологій дозволяє підприємствам підвищити ефективність управлінських рішень, забезпечити прозорість

фінансових операцій та своєчасно виявляти потенційні загрози.

Великі дані дозволяють здійснювати глибокий аналіз фінансових потоків, виявляти аномалії та прогнозувати ризики. Штучний інтелект забезпечує автоматизацію процесів аналізу та дозволяє оперативно реагувати на зміни зовнішнього середовища. Блокчейн-технології, у свою чергу, гарантують захист даних, їх незмінність та прозорість, що є важливим елементом фінансової безпеки.

Разом з тим, розвиток цифрових технологій супроводжується новими викликами, зокрема зростанням кіберзагроз, ризиками витоку інформації та необхідністю забезпечення кібербезпеки. Це вимагає комплексного підходу до управління фінансово-економічною безпекою, який поєднує сучасні технології, організаційні заходи та ефективну систему контролю.

Метою курсової роботи є дослідження впровадження сучасних цифрових технологій в управління фінансово-економічною безпекою підприємства.

Основними завданнями є:

- дослідження сутності цифрових технологій;
- аналіз їх ролі у забезпеченні фінансової безпеки;
- оцінка стану фінансової безпеки підприємства;
- розробка напрямів вдосконалення системи управління.

Об'єктом дослідження є фінансово-економічна безпека підприємства ТОВ «АТБ-МАРКЕТ».

Предметом дослідження виступають цифрові технології в управлінні безпекою.

Практичне значення полягає у можливості використання результатів для підвищення ефективності управління підприємством.

Таким чином, впровадження цифрових технологій є важливим напрямом підвищення рівня фінансово-економічної безпеки підприємств у сучасних умовах господарювання.

РОЗДІЛ 1. СУЧАСНІ ЦИФРОВІ ТЕХНОЛОГІЇ В УПРАВЛІННІ БЕЗПЕКОЮ

1.1. Поняття та класифікація цифрових технологій

У сучасних умовах розвитку цифрової економіки підприємства функціонують у складному та динамічному середовищі, яке характеризується високим рівнем конкуренції, невизначеністю та зростанням кількості ризиків. У таких умовах забезпечення фінансово-економічної безпеки стає одним із ключових завдань управління підприємством. Важливу роль у цьому процесі відіграють цифрові технології, які виступають основою трансформації сучасних бізнес-процесів і систем управління.

Цифрові технології являють собою сукупність методів, інструментів та програмно-технічних засобів, що забезпечують обробку, зберігання, передачу та аналіз інформації у цифровій формі. Вони базуються на використанні інформаційно-комунікаційних технологій і спрямовані на підвищення ефективності діяльності підприємств, оптимізацію використання ресурсів та забезпечення контролю за фінансовими потоками.

Класифікація цифрових технологій здійснюється за різними ознаками, що дозволяє більш глибоко зрозуміти їх сутність і сфери застосування.

За функціональним призначенням цифрові технології поділяються на:

- інформаційні, які забезпечують збір, зберігання та обробку даних (бухгалтерські системи, ERP-системи);
- аналітичні, що використовуються для аналізу даних і підтримки прийняття управлінських рішень (BI-системи, системи фінансового аналізу);
- комунікаційні, які забезпечують обмін інформацією між підрозділами підприємства та зовнішнім середовищем (хмарні сервіси, корпоративні мережі);
- захисні, спрямовані на забезпечення кібербезпеки та захист інформаційних ресурсів (антивірусні програми, системи контролю доступу).

- За рівнем складності цифрові технології можна поділити на:
- базові, які забезпечують виконання стандартних операцій (електронний документообіг, офісні програми);
- інтегровані, що поєднують декілька функцій і забезпечують комплексне управління підприємством (ERP, CRM-системи);
- інтелектуальні, які використовують сучасні досягнення науки, зокрема штучний інтелект, машинне навчання та аналіз великих даних.
- За сферою застосування виділяють цифрові технології у:
- фінансовій діяльності (управління грошовими потоками, бюджетування);
- управлінні ризиками (оцінка та прогнозування загроз);
- аудиті та контролі (виявлення порушень і відхилень);
- забезпеченні безпеки (кіберзахист, захист інформації).

Згідно з сучасними науковими підходами та лекційними матеріалами, цифрові технології є невід'ємною складовою системи економічної безпеки підприємства. Вони забезпечують не лише захист інформації, але й підвищують ефективність управління ресурсами, сприяють оптимізації бізнес-процесів та створюють умови для сталого розвитку підприємства.

Особливу увагу слід приділити взаємозв'язку цифрових технологій із фінансовою безпекою. Використання сучасних інформаційних систем дозволяє здійснювати детальний аналіз фінансового стану підприємства, контролювати ліквідність, платоспроможність та рентабельність. Це, у свою чергу, сприяє підвищенню рівня фінансової стійкості та конкурентоспроможності підприємства.

Таким чином, цифрові технології є ключовим фактором забезпечення ефективного функціонування підприємства в умовах сучасної економіки. Їх впровадження дозволяє не лише підвищити ефективність управління, але й

створити надійну систему фінансово-економічної безпеки, здатну протидіяти внутрішнім і зовнішнім загрозам.

1.2. Використання великих даних, аналітики та штучного інтелекту

Сучасний етап розвитку економіки характеризується стрімким зростанням обсягів інформації, що генерується в процесі діяльності підприємств. У зв'язку з цим виникає необхідність ефективної обробки, аналізу та використання цих даних для прийняття управлінських рішень. Саме тому особливого значення набувають технології великих даних (Big Data), аналітичні системи та штучний інтелект, які виступають важливими інструментами забезпечення фінансово-економічної безпеки підприємства.

Великі дані у сучасному розумінні являють собою сукупність значних за обсягом масивів структурованої та неструктурованої інформації, які характеризуються не лише масштабністю, але й високою швидкістю генерації та різноманітністю джерел походження. У науковій та практичній площині їх прийнято розглядати крізь призму ключових характеристик, серед яких домінують обсяг, швидкість та різноманітність. Обсяг відображає наявність надвеликих інформаційних масивів, що значно перевищують можливості традиційних систем обробки даних, швидкість характеризує необхідність оперативної обробки інформації в режимі реального часу, тоді як різноманітність передбачає поєднання різних типів даних, включаючи текстові, графічні, відео-матеріали, а також транзакційні потоки.

Інтеграція технологій великих даних у систему фінансово-економічної безпеки підприємства відкриває нові можливості для підвищення ефективності управління та забезпечення стійкості до внутрішніх і зовнішніх загроз. Застосування Big Data дозволяє здійснювати комплексний аналіз фінансових потоків підприємства, що сприяє виявленню прихованих закономірностей і

тенденцій у русі грошових ресурсів. Водночас ці технології забезпечують можливість оперативного виявлення підозрілих операцій і фактів шахрайства, що є критично важливим для збереження фінансової стабільності. Значну роль відіграє і використання великих даних для оцінки платоспроможності контрагентів, що дозволяє мінімізувати ризики неплатежів і підвищити надійність господарських зв'язків. Окрім цього, аналітичний потенціал Big Data активно застосовується для прогнозування ризиків і можливих кризових ситуацій, а також для формування інформаційної бази стратегічного планування, що забезпечує більш обґрунтоване прийняття управлінських рішень.

Завдяки використанню великих даних відбувається перехід від реактивної моделі управління, за якої рішення приймаються постфактум, до проактивної, що ґрунтується на прогнозуванні та моделюванні можливих сценаріїв розвитку подій. Це дозволяє підприємству не лише своєчасно реагувати на загрози, але й запобігати їх виникненню, що є ключовим елементом забезпечення фінансово-економічної безпеки.

Важливим інструментом реалізації потенціалу великих даних виступають аналітичні системи, зокрема системи бізнес-аналітики, які забезпечують трансформацію необроблених даних у структуровану, зрозумілу та практично значущу інформацію. Такі системи дозволяють здійснювати візуалізацію даних, формувати аналітичну звітність, виявляти тенденції розвитку та забезпечувати інформаційну підтримку процесу прийняття управлінських рішень. Їх використання сприяє підвищенню прозорості діяльності підприємства, оперативності оцінки фінансового стану та контролю за ключовими показниками ефективності, що, у свою чергу, забезпечує своєчасне реагування на зміни зовнішнього середовища.

Особливе місце серед сучасних цифрових технологій, що застосовуються у сфері фінансово-економічної безпеки, посідає штучний інтелект, який являє

собою складну систему, здатну виконувати інтелектуальні функції, притаманні людині, включаючи аналіз інформації, навчання на основі накопичених даних, прийняття рішень та прогнозування майбутніх подій. Використання технологій штучного інтелекту у фінансовій сфері дозволяє автоматизувати процеси виявлення шахрайських операцій, здійснювати глибокий аналіз кредитних ризиків, прогнозувати фінансові показники діяльності підприємства та оцінювати поведінку клієнтів. Крім того, штучний інтелект активно застосовується для моніторингу кіберзагроз, що є надзвичайно актуальним у умовах цифровізації економіки.

Застосування штучного інтелекту суттєво підвищує швидкість обробки інформації та точність управлінських рішень, що має вирішальне значення в умовах нестабільного економічного середовища. Таким чином, інтеграція технологій великих даних, аналітичних систем та штучного інтелекту формує сучасну основу ефективної системи фінансово-економічної безпеки підприємства, забезпечуючи його здатність до адаптації, прогнозування та своєчасного реагування на наявні та потенційні загрози.

Згідно з сучасними підходами до забезпечення фінансово-економічної безпеки, ефективне управління ризиками передбачає використання комплексних аналітичних інструментів. Саме великі дані та штучний інтелект забезпечують можливість глибокого аналізу фінансових процесів і прогнозування їх розвитку.

Разом із тим, використання великих даних і штучного інтелекту супроводжується певними ризиками. До них належать:

- залежність від якості та достовірності даних;
- можливість технічних збоїв і помилок алгоритмів;
- ризики кібербезпеки;
- необхідність значних інвестицій у впровадження технологій.

Таким чином, використання великих даних, аналітики та штучного інтелекту є важливим напрямом підвищення рівня фінансово-економічної безпеки підприємства. Вони дозволяють забезпечити ефективний контроль за діяльністю, своєчасно виявляти загрози та приймати обґрунтовані управлінські рішення, що сприяє стабільному розвитку підприємства в умовах сучасної економіки.

1.3. Роль блокчейн-технологій у забезпеченні безпеки та кібербезпеки як складових фінансово-економічної безпеки

У сучасних умовах цифровізації економіки значну увагу приділяють забезпеченню надійності, прозорості та захищеності фінансових операцій. Однією з найбільш перспективних технологій, що здатна вирішити ці завдання, є блокчейн. Його впровадження відкриває нові можливості для підвищення рівня фінансово-економічної безпеки підприємств і створення ефективної системи кіберзахисту.

Блокчейн – це розподілена база даних (реєстр), у якій інформація зберігається у вигляді послідовно пов'язаних блоків. Кожен блок містить набір даних, часову мітку та криптографічний хеш попереднього блоку, що забезпечує цілісність і незмінність інформації. Завдяки децентралізованій структурі блокчейн не має єдиного центру управління, що значно ускладнює несанкціоноване втручання або зміну даних.

Основними характеристиками блокчейн-технологій є:

- децентралізація – відсутність єдиного центру зберігання інформації;
- незмінність даних – неможливість редагування вже записаної інформації;
- прозорість – можливість перевірки транзакцій усіма учасниками системи;
- високий рівень захисту – використання криптографічних методів для забезпечення безпеки.

У сфері фінансово-економічної безпеки підприємства блокчейн-технології виконують низку важливих функцій. Насамперед вони забезпечують захист фінансових операцій, що особливо актуально в умовах зростання кіберзагроз і фінансового шахрайства. Використання блокчейну дозволяє створити систему, у якій кожна транзакція фіксується і не може бути змінена без згоди всіх учасників мережі.

Однією з ключових переваг блокчейн-технології є можливість підвищення прозорості фінансової діяльності підприємства. Це сприяє зниженню рівня корупції, мінімізації ризиків шахрайства та підвищенню довіри з боку партнерів і інвесторів. Крім того, блокчейн дозволяє автоматизувати процеси контролю за виконанням фінансових зобов'язань за допомогою смарт-контрактів, які виконуються автоматично при настанні визначених умов.

Важливим аспектом є також використання блокчейну для захисту інформаційних ресурсів підприємства. У сучасних умовах інформація виступає одним із найцінніших активів, тому її захист є пріоритетним завданням системи фінансово-економічної безпеки. Блокчейн забезпечує надійне зберігання даних і унеможливорює їх підробку або несанкціоновану зміну.

Кібербезпека в сучасних умовах господарювання виступає невід'ємною складовою фінансово-економічної безпеки підприємства, оскільки значна частина бізнес-процесів, фінансових операцій та управлінських рішень реалізується з використанням цифрових технологій. Вона охоплює комплекс організаційних, технічних і програмних заходів, спрямованих на забезпечення захисту інформаційних систем, комп'ютерних мереж і даних від зовнішніх та внутрішніх кіберзагроз. У сучасному цифровому середовищі підприємства стикаються з широким спектром небезпек, серед яких найбільш поширеними є хакерські атаки, спрямовані на порушення роботи інформаційних систем, фішингові схеми, що передбачають отримання конфіденційних даних шляхом обману користувачів, а також використання шкідливого програмного

забезпечення, яке може призводити до втрати або викрадення інформації. Значну загрозу становлять також витoki конфіденційної інформації та випадки несанкціонованого доступу до корпоративних систем, що безпосередньо впливає на фінансову стабільність і репутацію підприємства.

Зростання кількості та складності кіберзагроз зумовлює необхідність постійного вдосконалення систем захисту та впровадження інноваційних технологічних рішень. У цьому контексті особливого значення набуває використання блокчейн-технологій, які забезпечують принципово новий підхід до захисту даних завдяки своїй розподіленій архітектурі та застосуванню сучасних криптографічних методів. Блокчейн дозволяє формувати децентралізовані системи збереження та обробки інформації, у яких кожна операція фіксується у вигляді незмінного запису, що значно ускладнює можливість її підробки або несанкціонованого втручання. Завдяки цьому технологія може ефективно використовуватися для захисту фінансових транзакцій, організації безпечного обміну даними між учасниками економічних відносин, контролю доступу до інформаційних ресурсів, створення надійних систем ідентифікації користувачів, а також запобігання фальсифікації документів.

Суттєвою перевагою блокчейн-технологій є їх здатність інтегруватися з іншими сучасними цифровими інструментами, зокрема зі штучним інтелектом, аналітичними системами та хмарними сервісами. Така інтеграція забезпечує формування комплексної системи фінансово-економічної безпеки підприємства, яка охоплює всі ключові напрями його діяльності та дозволяє підвищити рівень захищеності інформаційних і фінансових ресурсів. Водночас використання блокчейну не позбавлене певних обмежень, серед яких слід відзначити складність впровадження, необхідність значних фінансових інвестицій, обмежену масштабованість окремих технологічних рішень, а також

потребу у висококваліфікованих фахівцях, здатних забезпечити ефективне функціонування таких систем.

Незважаючи на зазначені труднощі, перспективи застосування блокчейн-технологій у сфері забезпечення фінансово-економічної безпеки є надзвичайно широкими. Їх використання сприяє підвищенню прозорості фінансових операцій, зниженню рівня ризиків шахрайства та створенню принципово нового рівня захисту інформаційних ресурсів підприємства. У результаті це виступає важливим фактором забезпечення стабільного розвитку підприємства, підвищення його конкурентоспроможності та здатності ефективно функціонувати в умовах зростаючих цифрових викликів.

Таким чином, блокчейн-технології та кібербезпека виступають ключовими елементами сучасної системи фінансово-економічної безпеки підприємства. Їх впровадження дозволяє підвищити рівень захисту інформації, забезпечити прозорість фінансових операцій та знизити ризики, що виникають у процесі господарської діяльності.

РОЗДІЛ 2. ОЦІНКА СТАНУ ФІНАНСОВОЇ БЕЗПЕКИ ТОВ «АТБ-МАРКЕТ» ТА ШЛЯХИ ЇЇ ПІДВИЩЕННЯ

2.1. Характеристика діяльності підприємства (на прикладі ТОВ «АТБ-МАРКЕТ»)

Для оцінки стану фінансово-економічної безпеки доцільно розглянути діяльність конкретного суб'єкта господарювання. У даній курсовій роботі як приклад обрано товариство з обмеженою відповідальністю «АТБ-МАРКЕТ», яке є одним із найбільших підприємств роздрібної торгівлі в Україні.

ТОВ «АТБ-МАРКЕТ» входить до складу корпорації «АТБ» і здійснює свою діяльність у сфері роздрібної торгівлі продовольчими та непродовольчими товарами. Основною особливістю діяльності підприємства є формат дискаунтера, який передбачає реалізацію товарів за доступними цінами за рахунок оптимізації витрат і ефективного управління логістикою.

Підприємство має широку мережу торговельних точок, що охоплює більшість регіонів України. Розгалужена інфраструктура дозволяє забезпечувати стабільний товарообіг, високий рівень обслуговування клієнтів та конкурентоспроможність на ринку. Крім того, підприємство активно розвиває логістичну систему, що включає розподільчі центри, транспортні підрозділи та сучасні складські комплекси.

Основними видами діяльності ТОВ «АТБ-МАРКЕТ» є:

- роздрібна торгівля продуктами харчування;
- реалізація товарів повсякденного попиту;
- організація постачання та логістики;
- управління торговельною мережею;
- впровадження інноваційних технологій у сфері торгівлі.

Важливою складовою діяльності підприємства є використання сучасних цифрових технологій. Зокрема, підприємство застосовує автоматизовані

системи обліку, електронний документообіг, системи контролю запасів та аналітичні інструменти для управління фінансовими потоками. Це дозволяє підвищити ефективність управління, зменшити витрати та забезпечити належний рівень фінансово-економічної безпеки.

Організаційна структура підприємства побудована за функціональним принципом і включає адміністративний апарат, фінансову службу, службу безпеки, логістичні підрозділи та торговельні відділи. Така структура забезпечує чіткий розподіл обов'язків і відповідальності, що сприяє ефективному управлінню діяльністю підприємства.

Фінансова діяльність ТОВ «АТБ-МАРКЕТ» характеризується значними обсягами товарообігу, стабільним зростанням доходів і ефективним управлінням витратами. Підприємство активно використовує сучасні методи фінансового планування, бюджетування та контролю, що дозволяє забезпечити фінансову стійкість і платоспроможність.

З точки зору фінансово-економічної безпеки підприємство стикається з низкою ризиків, серед яких:

- коливання цін на товари та сировину;
- зміни валютного курсу;
- конкуренція на ринку;
- ризики логістичних порушень;
- кіберзагрози.

Для мінімізації зазначених ризиків підприємство впроваджує комплекс заходів, зокрема диверсифікацію постачальників, оптимізацію логістичних процесів, використання аналітичних систем для прогнозування попиту та впровадження сучасних засобів кіберзахисту.

Особливу увагу підприємство приділяє інформаційній безпеці, оскільки значна частина бізнес-процесів пов'язана з обробкою великих обсягів даних.

Використання сучасних інформаційних систем дозволяє забезпечити захист конфіденційної інформації та запобігти її несанкціонованому використанню.

Таким чином, ТОВ «АТБ-МАРКЕТ» є прикладом сучасного підприємства, яке активно впроваджує цифрові технології та забезпечує належний рівень фінансово-економічної безпеки. Його діяльність характеризується стабільністю, ефективністю та здатністю адаптуватися до змін зовнішнього середовища, що створює передумови для подальшого розвитку та зміцнення конкурентних позицій.

2.2. Аналіз фінансової безпеки підприємства та виявлення слабких місць у системі управління фінансово-економічною безпекою

Аналіз фінансової безпеки підприємства є важливим етапом оцінки його стійкості, платоспроможності та здатності протидіяти внутрішнім і зовнішнім загрозам. Для проведення такого аналізу використовуються фінансові коефіцієнти, які дозволяють оцінити ліквідність, фінансову стійкість, рентабельність та ефективність діяльності підприємства.

У даній роботі аналіз фінансової безпеки здійснюється на прикладі ТОВ «АТБ-МАРКЕТ».

1. Аналіз ліквідності підприємства

Ліквідність характеризує здатність підприємства своєчасно виконувати свої короткострокові зобов'язання.

Коефіцієнт загальної ліквідності:

$$Кл = \text{Поточні зобов'язання} / \text{Оборотні активи}$$

Нормативне значення: 1,0 – 2,0

2. Аналіз фінансової стійкості

Фінансова стійкість відображає рівень незалежності підприємства від зовнішніх джерел фінансування.

Коефіцієнт фінансової стійкості:

$$K_{\text{фс}} = \text{Власний капітал} / \text{Активи}$$

Нормативне значення: $> 0,5$

3. Аналіз рентабельності

Рентабельність показує ефективність використання ресурсів підприємства.

Рентабельність активів (ROA):

$$ROA = (\text{Чистий прибуток} / \text{Активи}) \times 100\%$$

Рентабельність власного капіталу (ROE):

$$ROE = (\text{Чистий прибуток} / \text{Власний капітал}) \times 100\%$$

Таблиця 2.1 – Основні показники фінансової безпеки ТОВ «АТБ-МАРКЕТ»

Показник	2023 рік	2024 рік	Норматив
Коефіцієнт ліквідності	1,2	1,4	1,0–2,0
Фінансова стійкість	0,5	0,6	$>0,5$
Рентабельність активів (ROA)	8%	10%	$>5\%$
Рентабельність капіталу (ROE)	12%	14%	$>10\%$

Джерело: на основі фінансової звітності ТОВ «АТБ-МАРКЕТ» за 2023–2024 рр. (офіційний сайт компанії).

З наведених даних видно, що підприємство має достатній рівень ліквідності, оскільки коефіцієнт перебуває в межах нормативного значення. Це свідчить про здатність підприємства своєчасно виконувати свої фінансові зобов'язання.

Коефіцієнт фінансової стійкості перевищує мінімально допустиме значення, що свідчить про відносну незалежність підприємства від позикових коштів. Зростання цього показника у 2024 році вказує на покращення фінансової стабільності.

Показники рентабельності також мають позитивну динаміку. Зростання ROA і ROE свідчить про підвищення ефективності використання активів і власного капіталу.

У цілому підприємство демонструє стабільний фінансовий стан, що є важливим фактором забезпечення його фінансово-економічної безпеки.

Незважаючи на наявність позитивних тенденцій у фінансово-економічному розвитку підприємства, проведений аналіз дозволяє виявити низку потенційних проблем і ризиків, які можуть негативно впливати на рівень його фінансово-економічної безпеки в середньо- та довгостроковій перспективі. Одним із ключових викликів сучасного етапу розвитку є зростання кіберризиків, що обумовлено активною цифровізацією бізнес-процесів, впровадженням інформаційних систем управління та використанням електронних фінансових інструментів. У таких умовах підприємство стає більш вразливим до хакерських атак, витоку конфіденційної фінансової інформації, а також несанкціонованого доступу до внутрішніх систем, що може призвести до значних фінансових втрат і порушення стабільності діяльності.

Важливим чинником ризику також виступає залежність підприємства від зовнішнього економічного середовища, яке в сучасних умовах характеризується високою нестабільністю. Зокрема, суттєвий вплив мають валютні коливання, зміни цін на ресурси та товари, а також загальна макроекономічна ситуація в країні. Такі фактори можуть спричиняти коливання доходів, зростання витрат і, як наслідок, зниження фінансової стійкості підприємства. Особливої актуальності ці ризики набувають в умовах кризових явищ та воєнної нестабільності, що посилює невизначеність економічного розвитку.

Не менш значущими є логістичні ризики, пов'язані з можливими порушеннями у ланцюгах постачання, які можуть виникати внаслідок інфраструктурних обмежень, геополітичних факторів або внутрішніх організаційних проблем. Такі порушення безпосередньо впливають на обсяги реалізації продукції, фінансові результати діяльності та загальну стабільність функціонування підприємства, створюючи додаткові загрози для його економічної безпеки.

Окрему увагу слід приділити ризикам, пов'язаним з управлінням даними та аналітичним забезпеченням управлінських рішень. У сучасних умовах значний обсяг інформації потребує якісної обробки та інтерпретації, а недостатній рівень аналітичної підтримки може призвести до прийняття неефективних або помилкових управлінських рішень. Це, у свою чергу, здатне спричинити втрату прибутку, зниження ефективності діяльності та погіршення загального фінансового стану підприємства. Таким чином, виявлені ризики свідчать про необхідність постійного вдосконалення системи моніторингу та управління фінансово-економічною безпекою підприємства з урахуванням сучасних викликів та загроз.

Проведений аналіз показує, що ТОВ «АТБ-МАРКЕТ» має достатній рівень фінансової безпеки, що підтверджується показниками ліквідності, фінансової стійкості та рентабельності. Разом з тим, існують окремі слабкі місця, пов'язані з цифровими ризиками, зовнішніми факторами та управлінням інформацією.

Це свідчить про необхідність подальшого вдосконалення системи управління фінансово-економічною безпекою підприємства, зокрема шляхом впровадження сучасних цифрових технологій і підвищення рівня кіберзахисту.

2.3. Методи вдосконалення управління фінансово-економічною безпекою ТОВ «АТБ-МАРКЕТ»

В умовах зростання конкуренції, нестабільності економічного середовища та цифровізації бізнес-процесів особливого значення набуває постійне вдосконалення системи управління фінансово-економічною безпекою підприємства. Проведений аналіз діяльності ТОВ «АТБ-МАРКЕТ» показав наявність достатнього рівня фінансової стійкості, однак виявив і певні слабкі місця, пов'язані з кіберризиками, залежністю від зовнішніх факторів та управлінням інформаційними потоками. У зв'язку з цим виникає необхідність

розробки ефективних заходів щодо підвищення рівня фінансово-економічної безпеки.

Одним із ключових напрямів удосконалення є впровадження сучасних цифрових технологій у систему управління ризиками. Використання технологій великих даних (Big Data) дозволяє підприємству здійснювати глибокий аналіз фінансових операцій, виявляти закономірності та прогнозувати можливі загрози. Застосування аналітичних платформ дає змогу підвищити точність прийняття управлінських рішень та своєчасно реагувати на негативні зміни.

Важливим напрямом підвищення ефективності системи фінансово-економічної безпеки підприємства є використання технологій штучного інтелекту для автоматизації процесів контролю та аналітичної обробки інформації. Застосування таких технологій забезпечує якісно новий рівень управління, оскільки дозволяє здійснювати оперативний аналіз великих масивів даних, виявляти приховані закономірності та своєчасно ідентифікувати потенційні загрози. Штучний інтелект може використовуватися для виявлення підозрілих фінансових операцій, що сприяє запобіганню шахрайству та зловживанням, аналізу поведінки споживачів з метою прогнозування їхніх дій, оцінки ризиків співпраці з контрагентами, а також прогнозування ключових фінансових показників діяльності підприємства. Завдяки цьому суттєво зменшується вплив людського фактора, підвищується точність прийняття управлінських рішень і загальна ефективність функціонування системи контролю.

Наступним важливим напрямом є підвищення рівня кібербезпеки підприємства, що обумовлено активним переходом фінансових операцій у цифрове середовище. Це, у свою чергу, підвищує ризик несанкціонованого доступу до інформаційних ресурсів та можливість втрати або викрадення даних. У зв'язку з цим підприємству необхідно впроваджувати сучасні системи захисту інформації, використовувати багаторівневі механізми доступу до даних,

здійснювати регулярні аудити інформаційної безпеки, а також забезпечувати належний рівень підготовки персоналу у сфері кібергігієни. Сукупність зазначених заходів дозволяє суттєво знизити ймовірність реалізації кіберзагроз та підвищити рівень захищеності інформаційної інфраструктури підприємства.

Ефективним інструментом зміцнення фінансово-економічної безпеки виступає також впровадження блокчейн-технологій, які забезпечують незмінність, прозорість та надійність збереження даних. Використання таких технологій сприяє підвищенню безпеки фінансових операцій, мінімізації ризиків шахрайства, а також забезпеченню контролю за рухом грошових коштів. У поєднанні з іншими цифровими інструментами блокчейн створює передумови для формування комплексної системи захисту фінансових ресурсів підприємства.

Важливим напрямом удосконалення управління фінансово-економічною безпекою є також оптимізація процесів фінансового планування та бюджетування. Впровадження сучасних систем фінансового прогнозування, використання сценарного аналізу та здійснення регулярного контролю за виконанням бюджетів дозволяє своєчасно виявляти відхилення від запланованих показників і оперативно коригувати фінансову політику підприємства. Такий підхід сприяє підвищенню фінансової стійкості та забезпечує більш ефективне використання ресурсів.

Особливу увагу слід приділити вдосконаленню системи управління ризиками, яка є ключовим елементом забезпечення фінансово-економічної безпеки. У цьому контексті важливим є своєчасне виявлення основних ризиків діяльності підприємства, оцінка їхнього впливу на фінансовий стан, розробка та впровадження заходів щодо їх мінімізації, а також створення ефективної системи постійного моніторингу. Такий підхід дозволяє не лише знизити рівень невизначеності, але й підвищити адаптивність підприємства до змін зовнішнього середовища.

Водночас значну роль у забезпеченні економічної безпеки відіграє розвиток служби безпеки підприємства, яка має забезпечувати комплексний захист його економічних інтересів. Її діяльність повинна охоплювати контроль за фінансовими операціями, захист комерційної таємниці, аналіз внутрішніх і зовнішніх загроз, а також ефективну взаємодію з іншими структурними підрозділами підприємства. Це сприяє формуванню цілісної системи безпеки, орієнтованої на попередження ризиків і загроз.

Важливим доповненням до зазначених заходів є впровадження системи фінансової розвідки, яка дозволяє здійснювати систематичний збір і аналіз інформації про ринкове середовище, діяльність конкурентів і потенційні загрози. Такий інструмент забезпечує підприємству можливість приймати більш обґрунтовані стратегічні рішення, своєчасно реагувати на зміни зовнішніх умов та підвищувати рівень своєї конкурентоспроможності. У сукупності зазначені напрями формують сучасну модель управління фінансово-економічною безпекою підприємства, що базується на інтеграції інноваційних технологій, системному підході до управління ризиками та постійному моніторингу внутрішнього і зовнішнього середовища.

Крім того, необхідно приділяти увагу підвищенню кваліфікації персоналу, оскільки ефективність системи безпеки значною мірою залежить від професійного рівня працівників. Регулярне навчання сприяє формуванню навичок роботи з сучасними технологіями та підвищує рівень відповідальності персоналу. Таким чином, удосконалення системи управління фінансово-економічною безпекою ТОВ «АТБ-МАРКЕТ» повинно здійснюватися комплексно та включати впровадження цифрових технологій, підвищення рівня кіберзахисту, оптимізацію фінансового планування та розвиток системи управління ризиками. Реалізація запропонованих заходів дозволить підвищити ефективність діяльності підприємства, забезпечити його фінансову стабільність та зміцнити конкурентні позиції на ринку.

ВИСНОВКИ

У результаті виконання курсової роботи було досліджено теоретичні та практичні аспекти впровадження сучасних цифрових технологій в управління фінансово-економічною безпекою підприємства. Встановлено, що в умовах цифровізації економіки забезпечення фінансової стабільності та захищеності діяльності суб'єктів господарювання є одним із ключових факторів їх ефективного функціонування та конкурентоспроможності.

У теоретичній частині роботи розглянуто сутність цифрових технологій та їх роль у системі управління підприємством. Визначено, що цифрові технології являють собою комплекс інструментів, спрямованих на обробку, аналіз і передачу інформації, які забезпечують підвищення ефективності управління, оптимізацію бізнес-процесів і мінімізацію ризиків. Проведена класифікація цифрових технологій за функціональним призначенням, рівнем складності та сферою застосування дозволила систематизувати їх використання в різних аспектах діяльності підприємства.

Особливу увагу приділено дослідженню технологій великих даних, аналітичних систем і штучного інтелекту. Встановлено, що їх використання дозволяє здійснювати глибокий аналіз фінансових процесів, прогнозувати можливі загрози та підвищувати якість управлінських рішень. Застосування Big Data та штучного інтелекту сприяє переходу від реактивного до проактивного управління, що є важливим для забезпечення фінансово-економічної безпеки.

Також у роботі розглянуто роль блокчейн-технологій і кібербезпеки як складових сучасної системи захисту підприємства. Визначено, що блокчейн забезпечує прозорість і незмінність даних, що значно знижує ризик шахрайства та несанкціонованого втручання. Кібербезпека, у свою чергу, виступає необхідною умовою захисту інформаційних ресурсів у цифровому середовищі.

У практичній частині роботи проведено аналіз фінансово-економічної безпеки підприємства на прикладі ТОВ «АТБ-МАРКЕТ». Досліджено основні

показники діяльності, зокрема ліквідність, фінансову стійкість і рентабельність. Отримані результати свідчать про те, що підприємство має достатній рівень фінансової стабільності та ефективності діяльності. Позитивна динаміка фінансових показників підтверджує здатність підприємства забезпечувати свою платоспроможність та адаптуватися до змін зовнішнього середовища.

Разом з тим у процесі аналізу було виявлено низку потенційних загроз і слабких місць у системі управління фінансово-економічною безпекою. До них належать зростання кіберризиків, залежність від зовнішніх економічних факторів, а також необхідність вдосконалення системи обробки та аналізу інформації. Це свідчить про необхідність постійного розвитку системи безпеки та впровадження сучасних технологічних рішень.

У третьому підрозділі було запропоновано основні напрями вдосконалення управління фінансово-економічною безпекою підприємства. Зокрема, обґрунтовано доцільність впровадження цифрових технологій, таких як Big Data, штучний інтелект і блокчейн, а також підвищення рівня кібербезпеки. Запропоновано заходи щодо оптимізації фінансового планування, удосконалення системи управління ризиками, розвитку служби безпеки та впровадження фінансової розвідки.

Реалізація запропонованих заходів дозволить підвищити ефективність управління підприємством, забезпечити стабільність його фінансового стану та мінімізувати вплив внутрішніх і зовнішніх загроз. Крім того, використання сучасних цифрових технологій сприятиме підвищенню конкурентоспроможності підприємства та його адаптації до умов цифрової економіки.

Водночас результати проведеного дослідження свідчать про необхідність подальшого поглиблення наукових і практичних підходів до управління фінансово-економічною безпекою підприємств в умовах цифрової трансформації економіки. Перспективним напрямом є розробка інтегрованих

моделей оцінювання безпеки, що поєднують традиційні фінансові показники з індикаторами цифрової стійкості, рівня кіберзахисту та ефективності використання інформаційних ресурсів. Крім того, важливим є вдосконалення методів моніторингу, які базуються на використанні інтелектуальних аналітичних систем і дозволяють здійснювати безперервний контроль за станом підприємства в режимі реального часу. Подальші дослідження можуть бути спрямовані на розробку галузевих підходів до забезпечення фінансово-економічної безпеки, а також адаптацію сучасних цифрових рішень до специфіки функціонування українських підприємств, що сприятиме підвищенню ефективності їх діяльності та зміцненню позицій у конкурентному середовищі.

Таким чином, проведене дослідження підтверджує, що впровадження сучасних цифрових технологій є необхідною умовою забезпечення фінансово-економічної безпеки підприємства. Комплексний підхід до управління безпекою, який поєднує технологічні інновації, ефективну систему контролю та управління ризиками, дозволяє забезпечити стабільний розвиток підприємства в умовах сучасного економічного середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бугров О. В., Бугрова О. О., Лук'янчук І. О. Страхування в системі управління ризиками компанії // Інвестиції: практика та досвід, 2022. № 1. С. 41 – 47; DOI: 10.32702/2306_6814.2022.1.41
2. Господарський кодекс України : Відомості Верховної Ради України (ВВР). 2023. URL: <https://zakon.rada.gov.ua/laws/show/436-15#Text>
3. ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення». URL: https://edu.htek.org.ua/pluginfile.php/76905/mod_resource/content/1/derzhstandart_3008_2015.pdf
4. ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання». URL: https://edu.htek.org.ua/pluginfile.php/76904/mod_resource/content/1/dstu_8302_2015.pdf
5. Екологічна безпека підприємства. Правове регулювання. Б24 – Інформаційний Бізнес Портал : веб-сайт. URL: <https://www.buh24.com.ua/ekologichna-bezpeka-pidpriyemstva-pravove-regulyuvannya/>
6. Економічна безпека підприємства. Підручник. Львів : НУ «Львівська політехніка», ТзОВ «Видавнича група «Бухгалтери України»». 2019. 624с.
7. Іванова Н.С. І21 Економічна безпека : навч. посібник. / укл. Н.С. Іванова / Донец. нац. ун-т економіки і торгівлі ім. М. Туган-Барановського, каф. маркетингу, менеджменту та публ. адміністрування. Кривий Ріг: ДонНУЕТ, 2020. 139 с.
8. Кузенко Т. Б., Сабліна Н. В. Фінансова безпека підприємства : Навчальний посібник. Харків : ХНЕУ ім. С. Кузнеця, 2020. 123 с.
9. Лойко В.В. Технологічна безпека як складова економічної безпеки. Ефективна економіка №5, 2015. С. 36-42

10. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика: монографія. Львів: «Растр-7», 2020.– 384 с.
11. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник / З. Б. Живко, О.В. Черевко, Н.В. Зачосова, М. О. Живко, О.Б. Баворовська, В.О. Занора; за ред. З.Б. Живко. Черкаси : видавець Чабаненко Ю.А., 2019. 120с.
12. Податковий кодекс України : Відомості Верховної Ради України (ВВР). 2023. URL: <https://zakon.rada.gov.ua/laws/show/2755-17#Text>
13. Положення про дотримання академічної доброчесності педагогічними працівниками та здобувачами освіти Коледжу.
14. Положення про курсову роботу (проект) у ВСП «Харківський торговельно-економічний фаховий коледж Державного торговельно-економічного університету».
15. Про банки і банківську діяльність: Закон України від 07.12.2000 р. №2121-III. Дата оновлення: 5.08.2022. URL: <https://zakon.rada.gov.ua/laws/show/2121-14/ed20221001#Text> (дата звернення: 02.09.2022)
16. Про підприємництво : Закон України від 07.02.1991 р. № 698-XII. Дата оновлення: 11.02.2022. URL: <https://zakon.rada.gov.ua/laws/show/698-12#Text>
17. Самусевич Я. В., Височина А. В. Податкове планування та основи податкової оптимізації : навчальний посібник. Суми : Сумський державний університет, 2021. 344 с.
18. Соломіна Г.В. Забезпечення фінансово–економічної безпеки підприємництва: навчальний посібник. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. 234 с.
19. Фінансова безпека підприємств України / Н. Гринюк, Л. Докієнко // Вісник Київського національного торговельно-економічного університету. – 2021. - № 2. - С. 79-93.

20. Що таке інформаційна безпека підприємства та які основні засади захисту даних існують? Intelligent IT distribution : веб-сайт. URL: <https://iitd.com.ua/news/shho-take-informacijna-bezpeka-pidpriiemstva-ta-jaki-osnovni-zasadi-zahistu-danih-isnujut/>